Актуальні питання протидії кіберзлочинності та торгівлі людьми.
Харків, 2017

# РОЗДІЛ 5.
# МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

**УДК 341.1.8**

**Вікторія Володимирівна АРЕНДАР,**
*слухач магістратури факультету № 3 Харківського національного університету внутрішніх справ*

**Андрій Васильович ВОЙЦІХОВСЬКИЙ,**
*кандидат юридичних наук, доцент, професор кафедри конституційного і міжнародного права факультету № 4 Харківського національного університету внутрішніх справ*

## КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА МІЖНАРОДНІЙ БЕЗПЕЦІ

Розвиток інформаційних технологій призвів до масового використання у всьому світі мережі Інтернет. Остання є не тільки важливою сполучною ланкою між різними світовими культурами, але й важливим інструментом для обміну політичної, економічної, торгової, споживчої інформації.

Число активних користувачів Інтернету невпинно зростає, чим користуються різні злочинні елементи з метою розширення свого впливу на суспільну свідомість, поширення насильницької інформації, провокаційних заяв і т.п. Тому, з появою мережі Інтернет виникла одна з найбільш небезпечних різновидів кіберзлочинності – кібертероризм.

Що стосується визначення кібертероризму, то міжнародна спільнота ще не сформувала єдиного розуміння. Баррі Коллін, старший науковий співробітник Каліфорнійського інституту безпеки та розвідки, в 1980 році вперше вжив термін «кібертероризм». Відтоді учені стали аналізувати його як явище. Представник ФБР США, агент М. Поллітт, визначив цей вид тероризму як «навмисні політично мотивовані атаки на інформаційні комп'ютерні системи, комп'ютерні програми і дані, виражені в застосуванні насильства по відношенню до цивільних цілей з боку субнаціональних груп або таємних агентів».

Кібертероризм представляє велику загрозу інформаційній безпеці держави. Адже кібератаки націлені не тільки на пасивний збір даних, але й на незаконне заволодіння фінансовою і секретною інформацією, на отримання несанкціонованого доступу до апаратури контролю над космічними приладами, си-

стемами водопостачання та розподілу електроенергії, ядерними електростанціями, воєнними комплексами та ін.

На сьогодні протидією кібертероризму на міжнародному рівні займаються окремі міжнародні організації. Це Підрозділ по боротьбі з тероризмом ОБСЄ і Інтерпол. У рамках у ЄС розпочав роботу Центр по боротьбі з кіберзлочинністю. Країничлени ЄС і європейські інституції мають намір підтримувати Центр по боротьбі з кіберзлочинністю для створення оперативних і аналітичних можливостей її розслідування і для співпраці з міжнародними партнерами [1, с.58].

Крім того, задля протидії різним проявам кіберзлочинності, НАТО створив Технічний центр Сил реагування на комп'ютерні інциденти (NCIRC). NCIRC розробляють умови співробітництва, які зрештою відкриють доступ до спеціальних знань в усіх сферах кібербезпеки, а також рекомендації щодо реагування НАТО на прохання країн Альянсу і партнерів про допомогу в захисті їхніх інформаційних і комунікаційних систем [2, с.182].

Для більш ефективної протидії кібертероризму Єврокомісія пропонує створити нове відомство ЄС з кібербезпеки, а також розробити і ввести в Європі єдину систему сертифікації, яка дозволить гарантувати безпеку використання товарів і послуг у цифровому середовищі. Нове відомство пропонується створити на основі вже наявного і розташованого в Афінах Європейського агентства мережної та інформаційної безпеки (Enisa), розширивши його і наділивши новими повноваженнями. «Кібератаки стали все частішими, більш глобальними, витонченими, і Європа має бути спроможною протистояти цим атакам цілодобово у всіх країнах ЄС», - комісар ЄС з цифрової економіки та суспільства Андрус Ансіп.

Єдину систему сертифікації пропонують поширити на побутові прилади, автомобілі та будь-які пристрої, здатні підключатися до Інтернету. Сертифікати допоможуть споживачам у Європі розпізнавати, чи відповідають товари, які вони планують придбати, європейським стандартам безпеки [3].

Таким чином, потрібно усвідомити, що для ефективної протидії кібертероризму потрібна плідна міжнародна співпраця багатьох країн світу як на державному рівні, так і на рівні співробітництва між урядовими організаціями та представниками бізнесу у сфері розповсюдження ІТ-технологій.

Першочерговими завданнями для світової спільноти ми вбачаємо в: постійному удосконаленні законодавства у сфері

інформаційної безпеки держав; систематичному збирання та аналізі даних про потенційні кібертерористичні загрози; розробці якісних технологій захисту від кібернападів; встановлення заборон на використання у різних сферах не захищеного належним чином програмного забезпечення; введення єдиної системи сертифікації на побутові прилади, автомобілі та будь-які пристрої, здатні підключатися до мережі Інтернет.

**Список використаних джерел:**

1. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни *Науковий вісник Національного університету державної податкової служби України (економіка, право)*. 2014. № 2. С.55-60.
2. Войціховський А. В. Діяльність НАТО у боротьбі з кіберзлочинністю // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності: матеріали міжн. наук.-практ. конф. (Харків, 12 лист. 2014 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків: Права людини, 2014. С. 181-184.
3. 3. В Євросоюзі створять відомство з кібербезпеки // Корреспондент.net. 19.09.2017. URL: http://ua.korrespondent.net/world/3887910-v-yevrosouizi-stvoriat-vidomstvo-z-kiberbezpeky (дата звернення: 28.10.2017).

*Одержано 30.10.2017*